Performance Metrics Progression

Grady Summers
VP, Strategic Solutions
Mandiant

Joshua Bartolomie
Director, Cyber Security Architecture
Exelis

Matthew Shaffer
Consultant, Strategic Solutions
Mandiant

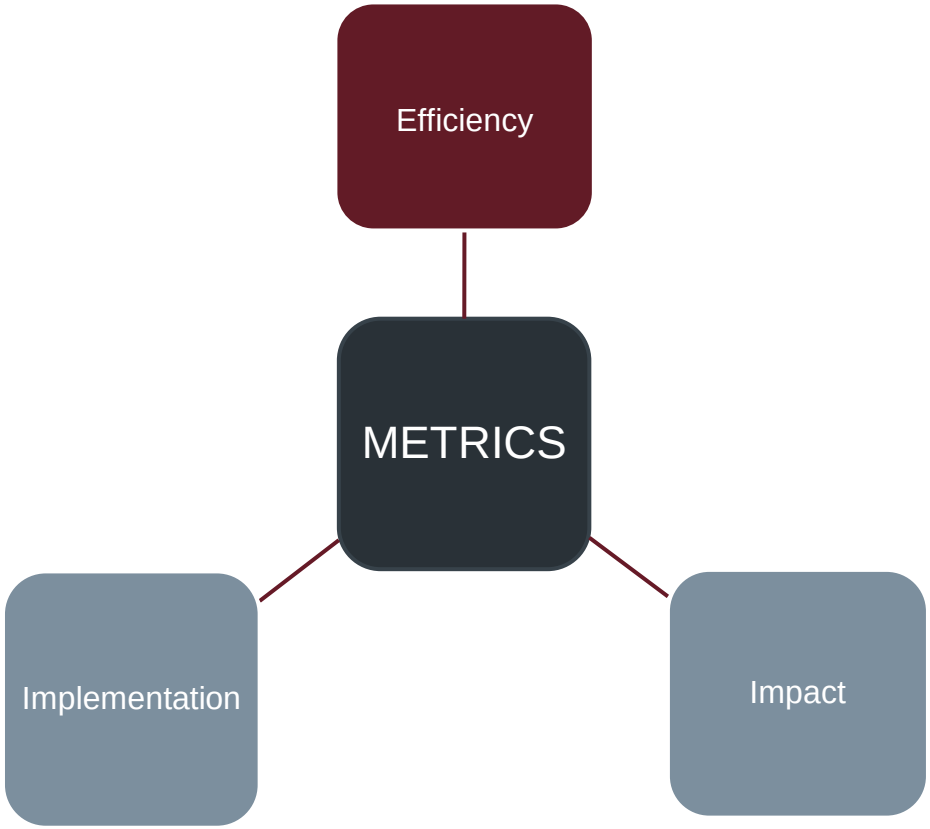
Briefing Structure and Goals

- Framework and Planning
  - Grady Summers – Vice President, Mandiant
  - Matthew Shaffer – Strategic Solutions Consultant, Mandiant
- Implementation and Utilization
  - Joshua Bartolomie – Director, Cyber Security Architecture, Exelis Inc.

MIRcon 2013

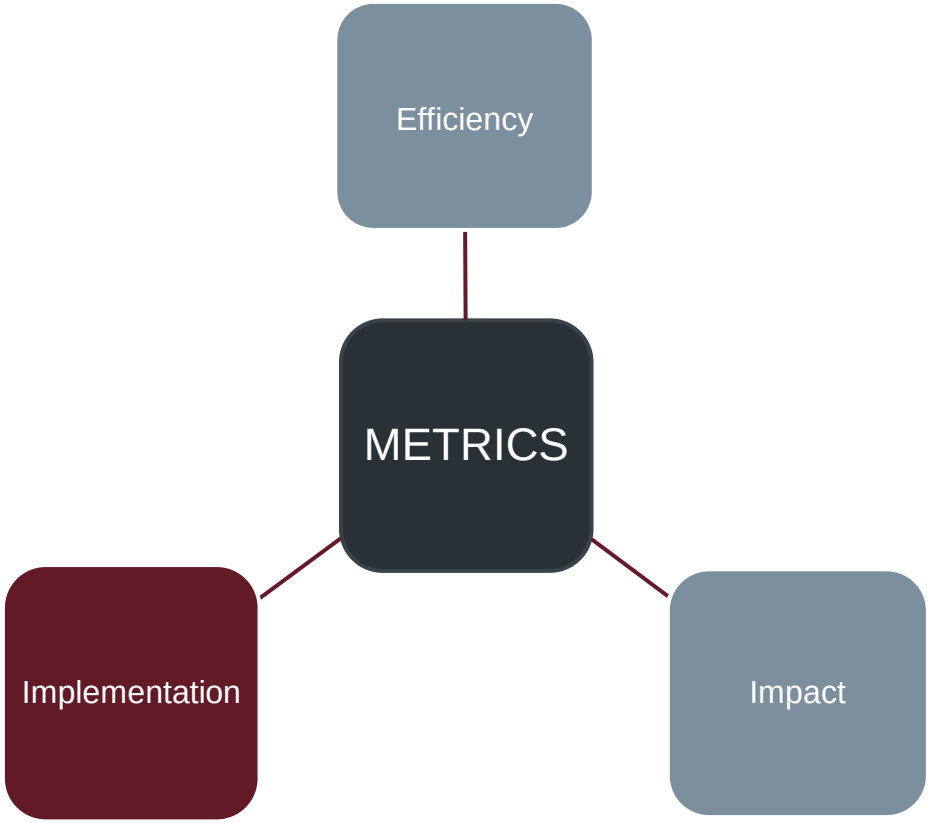
Efficiency Metrics

- Calculates effectiveness of monitoring and IR related people, process, and technology
- Typically CIRT internal
- Ex: DRAIN CVR



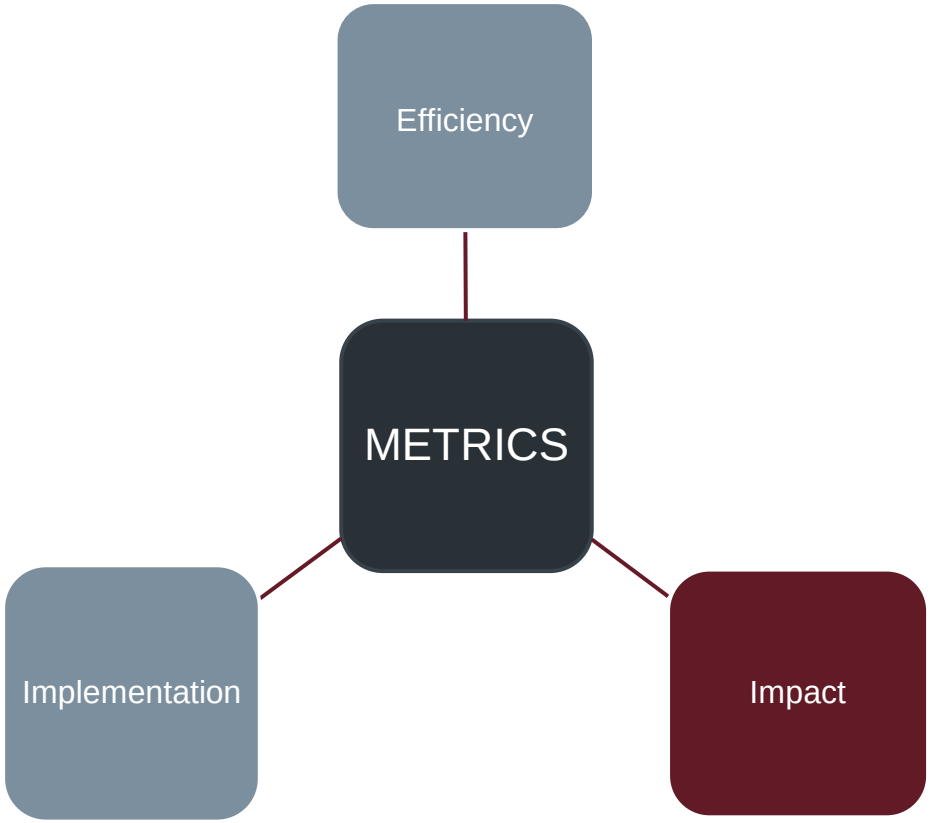
Implementation Metrics

- Calculates the progress of introducing new monitoring and IR related people, process, and technology
- Internally or externally focused
- Ex: Tracking successful technology deployment



Impact Metrics

- Calculates the impact that the CIRT has on the business
- Externally focused
- May utilize results of other metrics
- Ex: real dollar value in the percentage decrease in time to detect since management approved the budget for an additional full time analyst



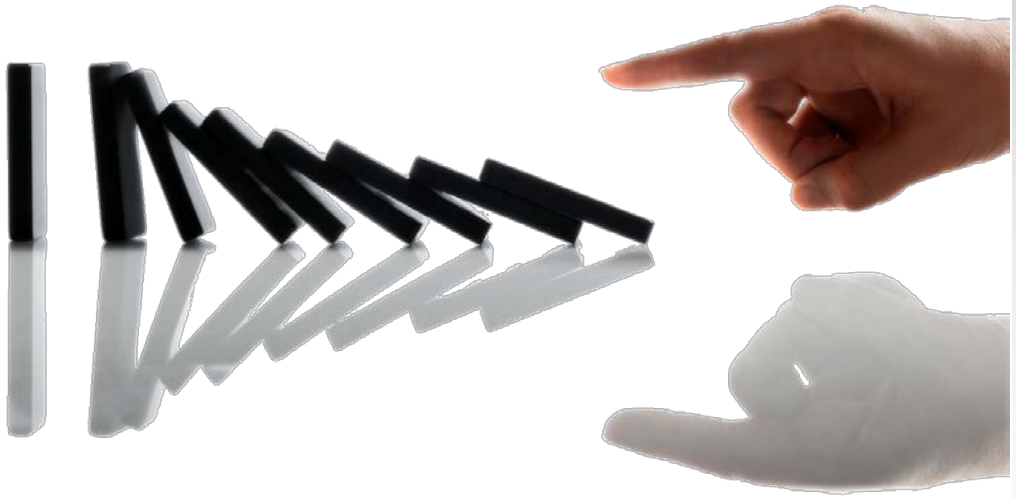
Proxy Metrics

- Use “proxy metrics” that are easily gathered in order to measure the hard-to-measure things you care about

You might not care about…	…but it’s a good way to measure
# of AV alerts per PC	Overall hygiene of environment
% of rogue/non-managed PCs on the network	Control over environment; prevalence of BYOD
Measuring every MS patch	Control over environment

Performance Metrics Plan

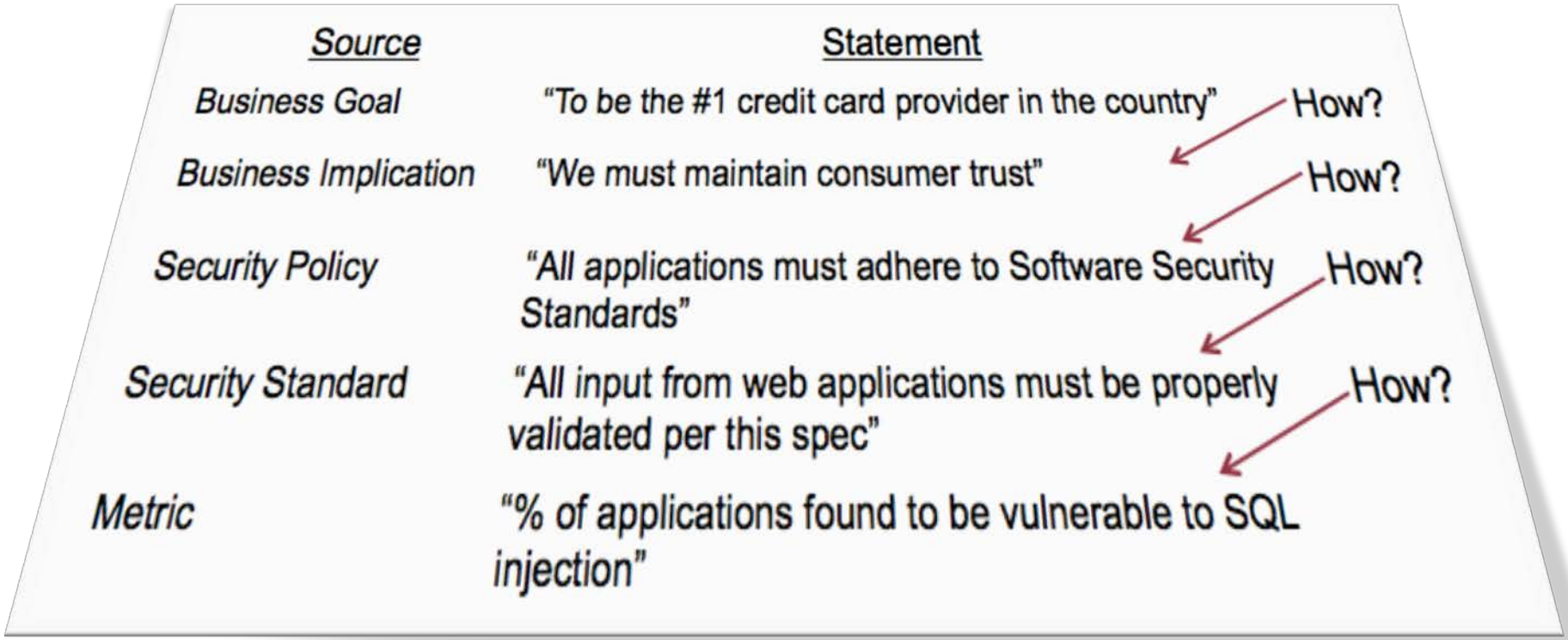
- A Performance Metrics Plan should:
  - Align with the CIRT Mission Statement
  - include a methodology
  - Identify stakeholders and reporting requirements



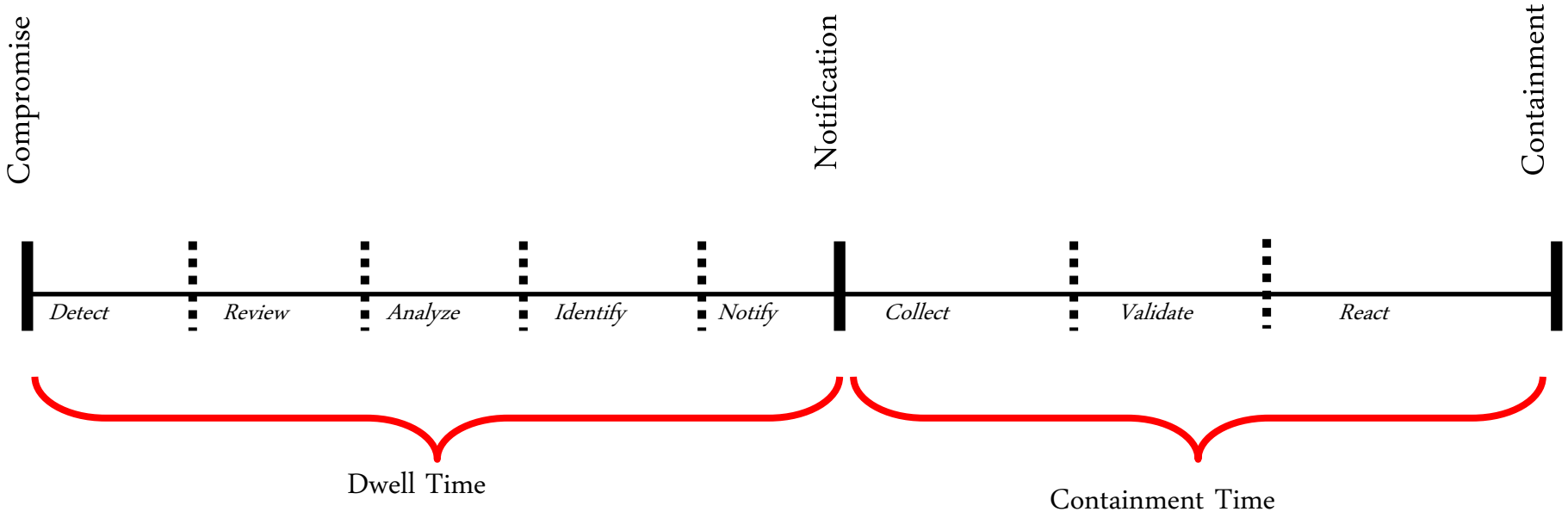
Determining What to Measure

- Quantifiable
- Flow requirements downhill
- Consider a focus rotation

Requirements Flow



DRAIN CVR - [dreyn kuhv-er] *noun.*



$$f\ ((D + R + A + I + N) + (C + V + R))$$

DRAIN & CVR Defined

D
R
A
I
N

C
V
R

Time	Category	Measurement	Benefit
Dwell	**Detect**	Time from initial entry into the system/network to detection	Measures the effectiveness of detection systems and capabilities
	Review	Time from detection to analyst to review the incident	Determine if staffing level is properly sized
	Analyze	Time to analyze the incident	Determines if the organization has the right expertise and tools and if the right escalation occurs
	Identify	Time to identify the affected assets, location, and owner	Measures the effectiveness of asset inventory
	Notify	Time to successfully notify appropriate contacts	Measures the effectiveness of contact database and communication plan
Containment	**Collect**	Time to collect live response data	Determines if there are the right tools deployed to assist in collection
	Validate	Time to validate intrusion based on collected data	Determines if the right skill sets are in place at each level
	React	Time to react (contain, remove, etc.)	Determines if there is the right definition of remediation and if it is applied consistently

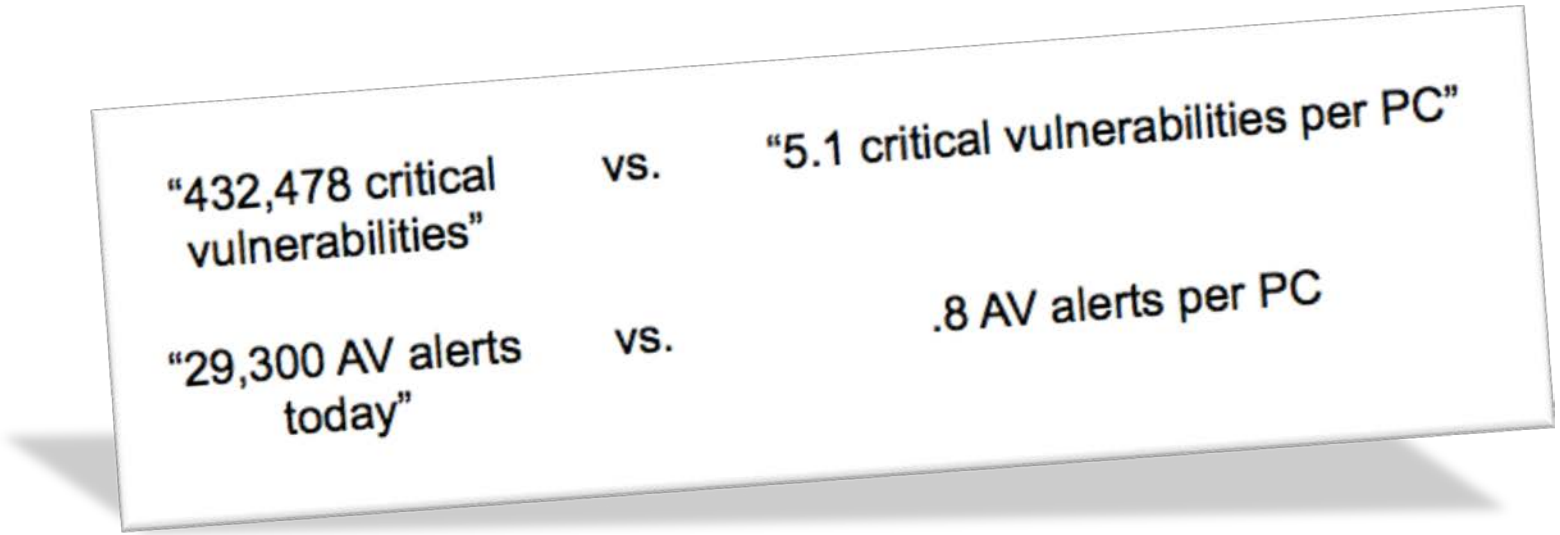
Reporting Template

- Documented and repeatable process
- Mission driven
- Consistent collection
- Communication

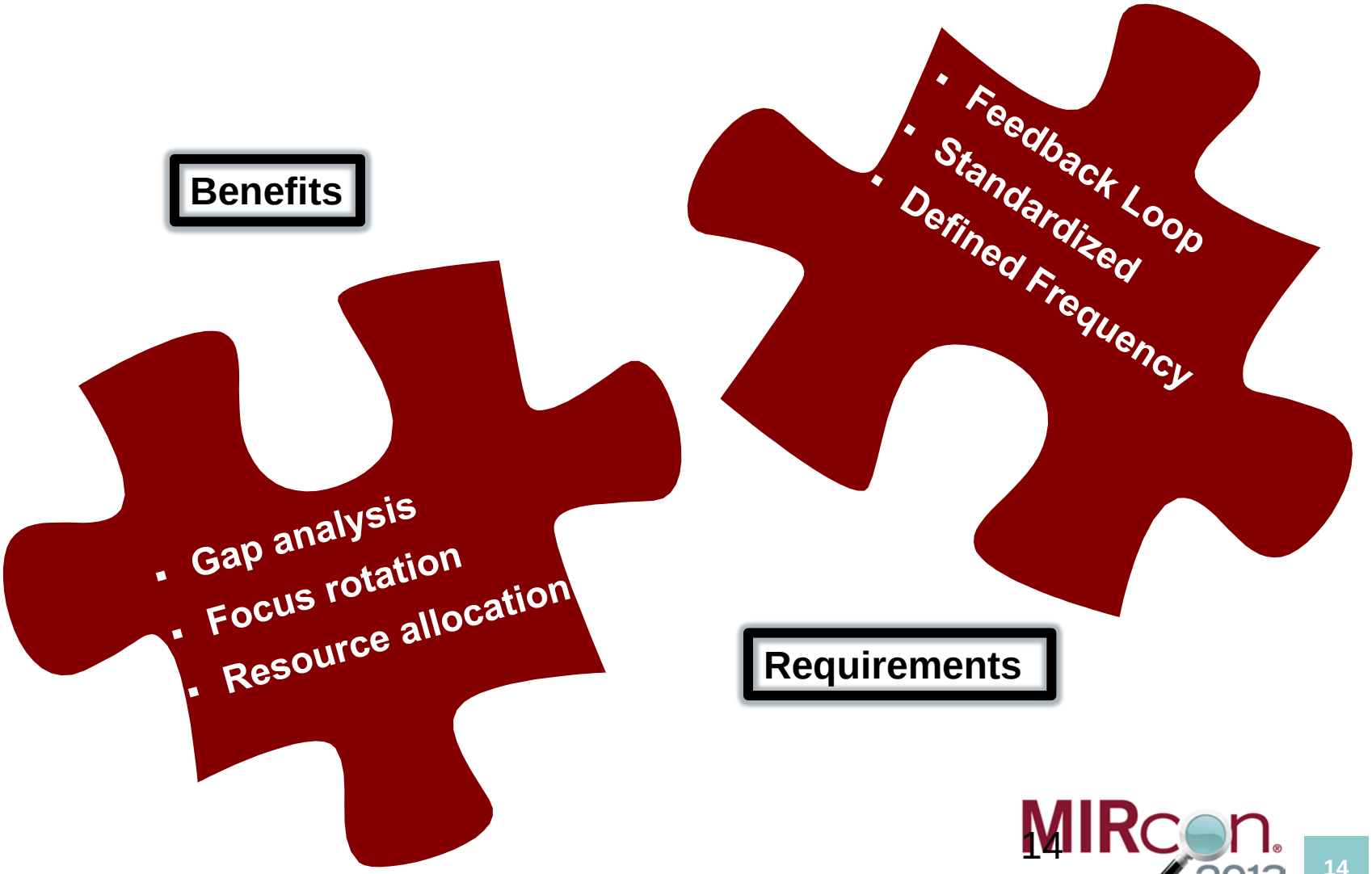
Field	Data
Metric	01 - Time to Detect
Reference Document	ACME SOP XYZ
Goal	Find the threat faster
Measure	Average hours to detect an incident from the moment of initial compromise
Formula	X = (Time to detect incident 1 + time to detect incident 2 + … time to detect incident n)/n
Objective	X < 8 hours
Frequency	Collection: Quarterly Reporting: Quarterly
Trend Retention	Three years
Responsible Stakeholder	SOC Manager
Data Source	Ticket system / Incident Reports
Reporting Format	Line Graph
Dissemination Mechanism	SOC Biannual Update

Reporting

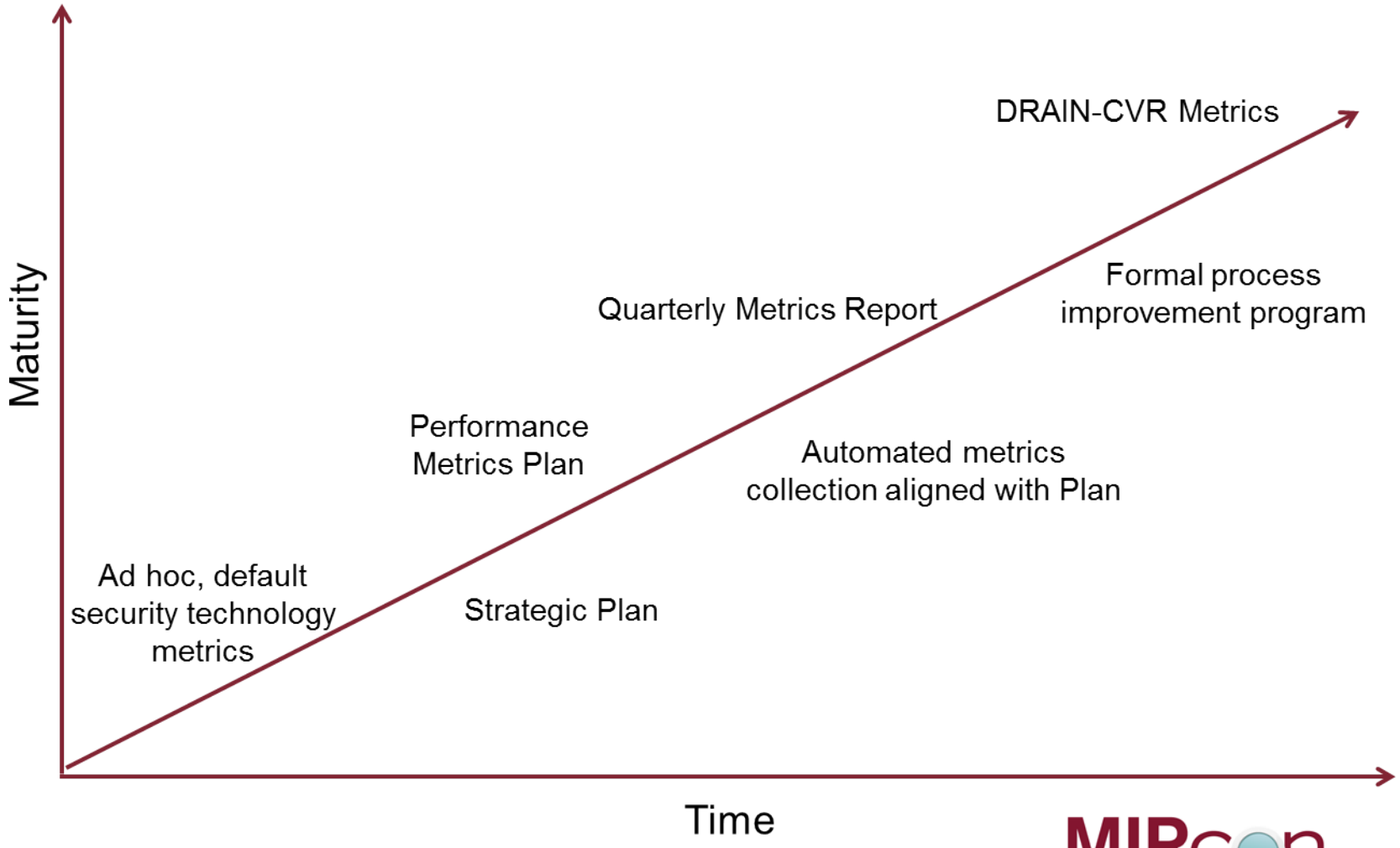
- Identify the appropriate audience
- Internal collection and external reporting may not adhere to the same frequency
- Report per-unit metrics where possible



Process Improvement



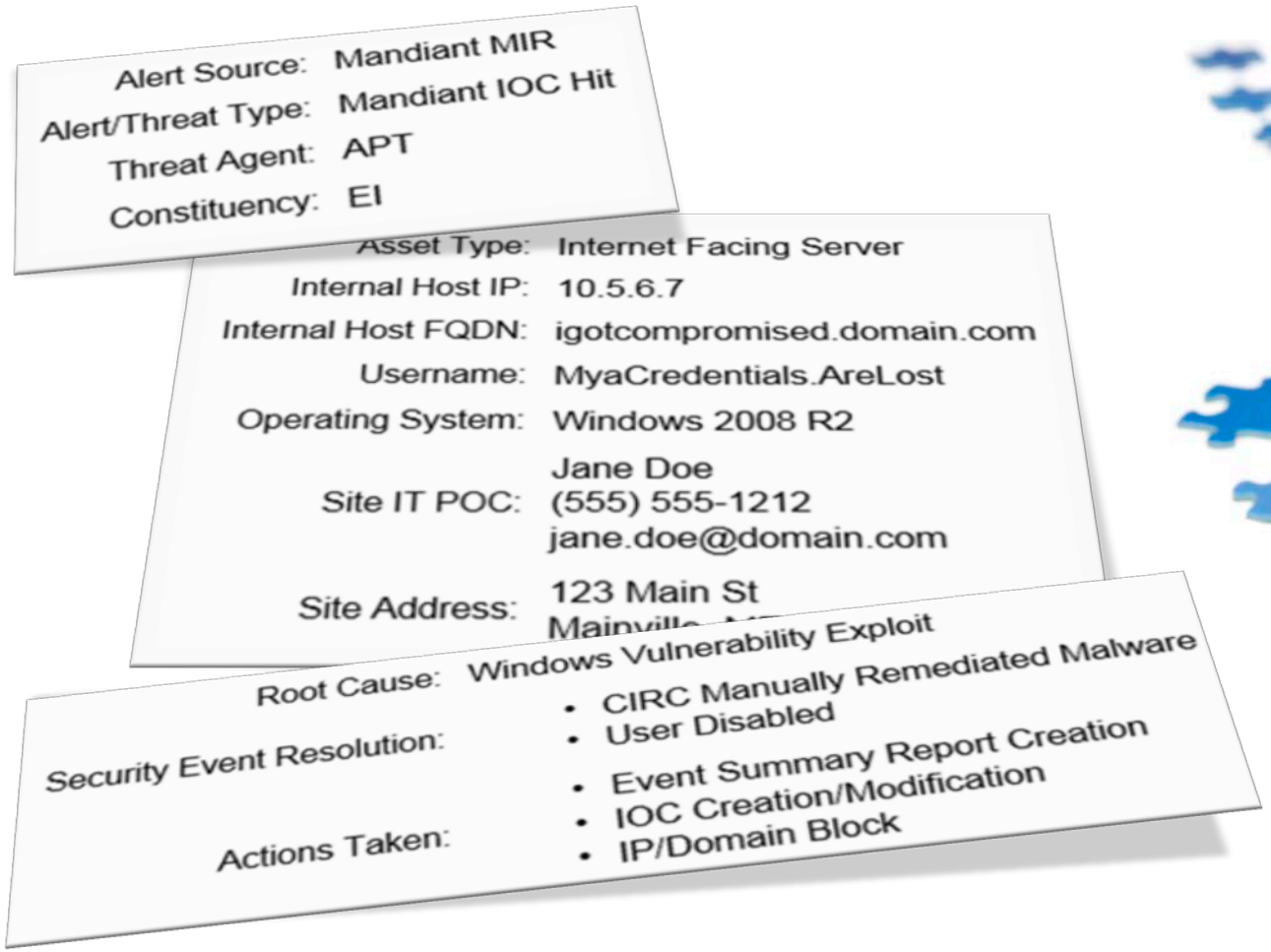
Key Milestones - Metrics

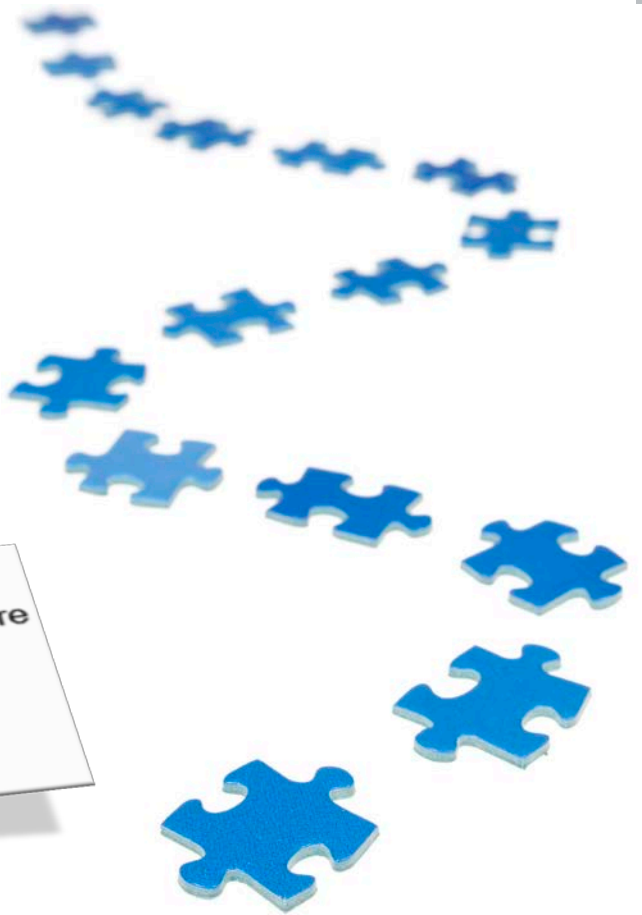


Putting Theory into Practice

- Open-minded communication
- Centralized documentation
- Maintain perspective
- Don’t wait for perfect

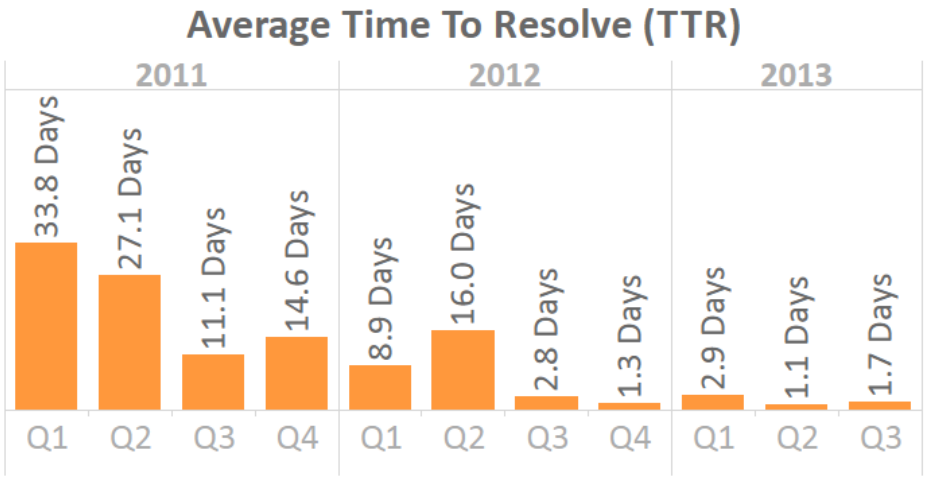
Security Event Instrumentation

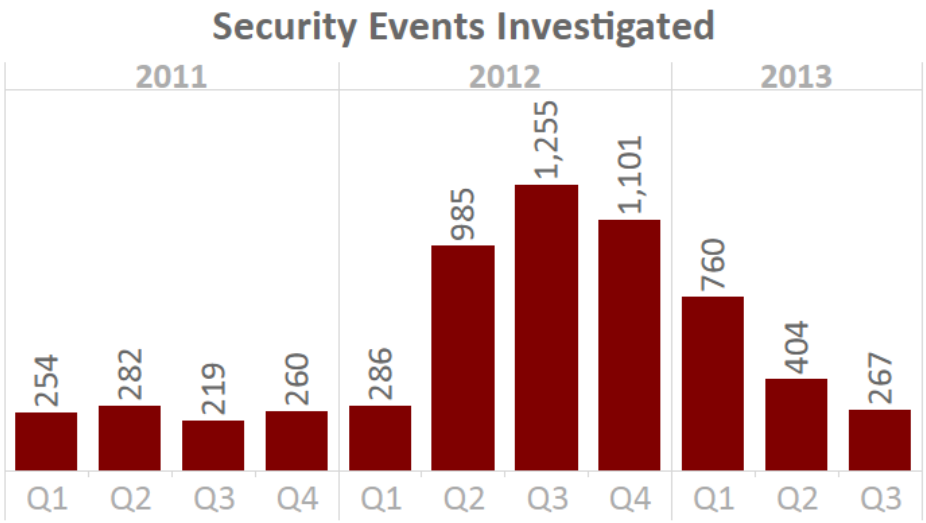


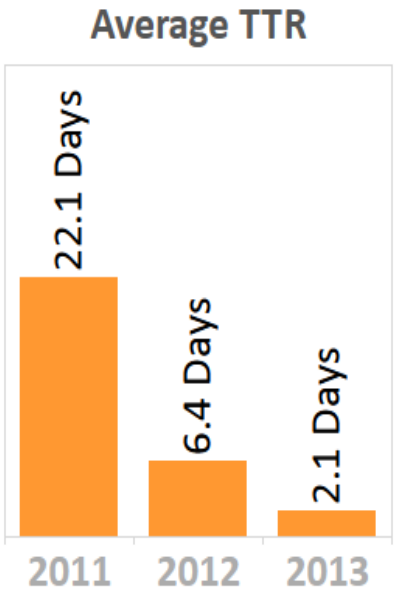


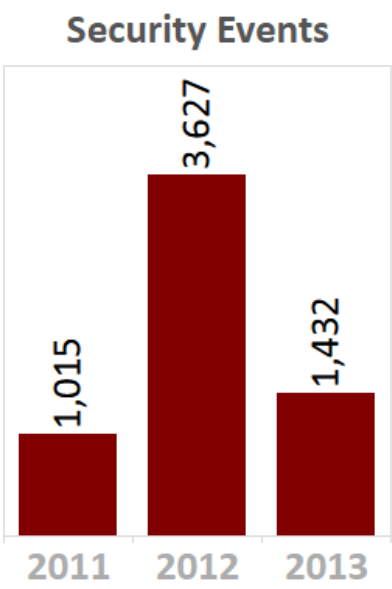
MIRcon 2013

IR Process Optimization

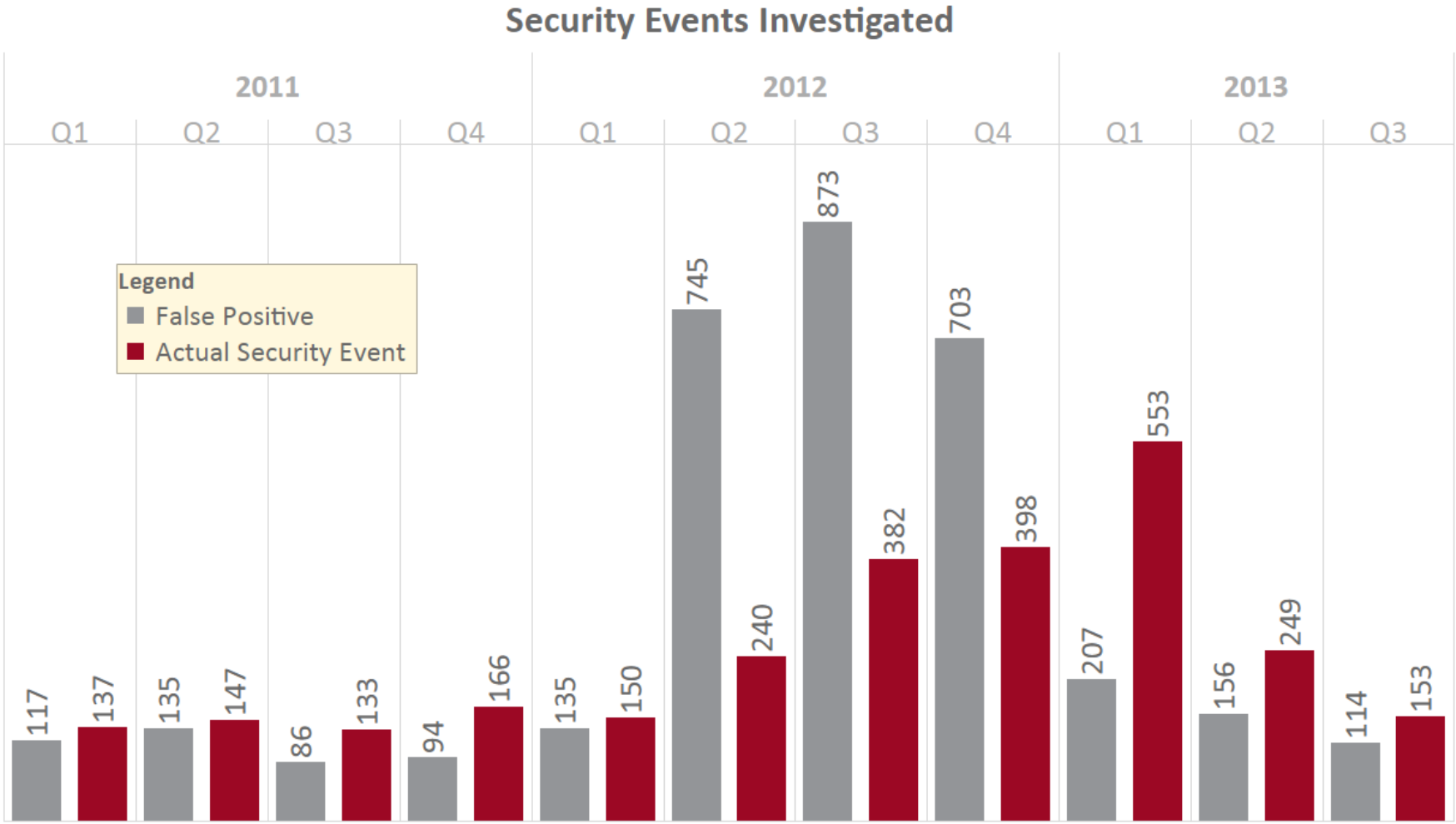




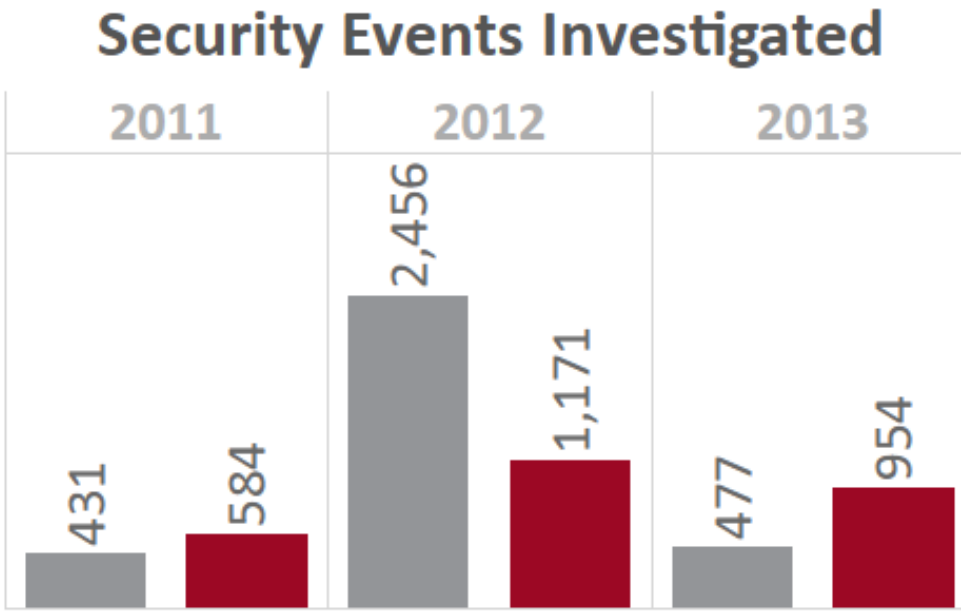


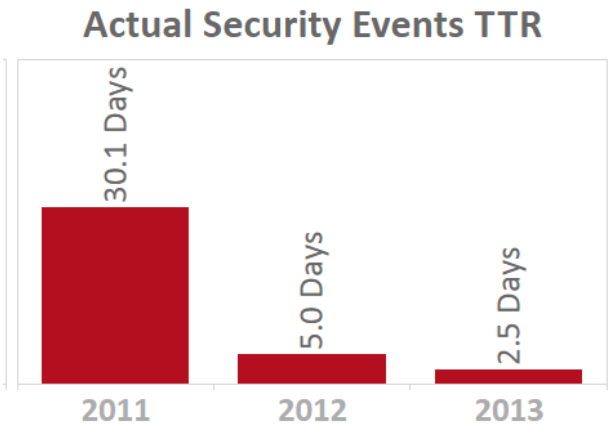


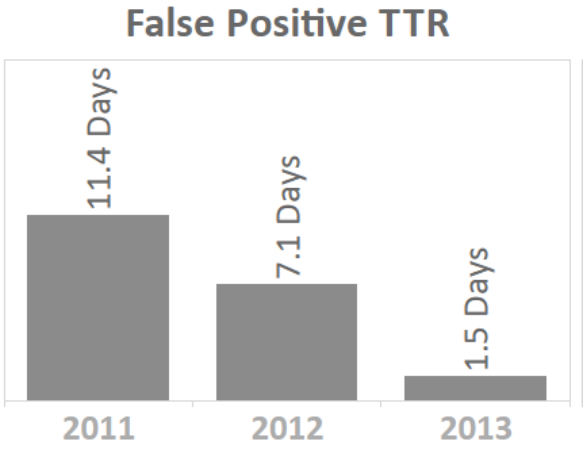
Process Optimization



Process Optimization







Security Posture and Threat Intelligence

Security Posture and Threat Intelligence

Executive Reporting

Executive Reporting

Questions

Grady Summers
Vice President | Mandiant Strategic Solutions
grady.summers@mandiant.com

Joshua Bartolomie
Director | Exelis Cyber Security Operations
joshua.bartolomie@exelisinc.com

Matthew Shaffer
Consultant | Mandiant Strategic Solutions
matthew.shaffer@mandiant.com

Appendix:
Example Security Event Data Points

- Event Data*
  - Alert Source**
  - Alert/Threat Type**
  - Constituency**
  - Asset Type**
  - Internal Host IP
  - Internal Host FQDN
  - Asset OS**
  - Threat Agent**
  - Threat Domains/IPs
  - Actions Taken**
  - Root Cause**
  - Resolution**
  - Targeted Attack**
  - Username
- Action Requests*
  - Evidence Collection**
  - Software Install/Upgrade**
  - Incident Reporting**
  - Analysis Assistance**
  - Malware Analysis**
  - Malware Submission
  - Network Block
  - Network Capture
  - Request Approval**

* Use a single record per individual unit of interest

** Predefined selections to ensure standardization